Summary Report[1]

Web-based Submission of the Discharge Monitoring Report[2]

EPA Contract #68-W5-0030[3]

Delivery Order #0004

Revised December 31, 1999

[1] Deliverables 10.1 and 10.2, InDyne, Inc. (formerly Information Dynamics, Inc.)

[2] A field test in the State of New York of the digital signing and submission of the Discharge Monitoring Report using an Adobe Acrobat Exchange plug-in to a Web browser as the electronic form environment which is connected interactively across the Internet to a receiving Web site. Cryptographic and handwritten biometric digital signatures are evaluated in this pilot.

[3] Submission of Environmental Data Under the Chinese Taipei Environmental Protection Administration-USEPA Technical Cooperation Agreement

1 Scope

This document summarizes experience with a pilot test of the Web-based submission of the New York State Discharge Monitoring Report (DMR) conducted in the State of New York June – November, 1999. Cryptographic digital signatures were evaluated in Phase 1 and biometric handwritten digital signatures were evaluated in Phase 2. Detailed design of the pilot, description of the commercial off-the-shelf software and hardware products used, test results, communications with the pilot participants and evaluations of Phase 1 and Phase 2 are contained in separate documents as shown in the following table.

Scope	Title
Software functions required for the pilot, and descriptions of commercial off-the-shelf software selected to fulfill these functions	Requirements Document
Overall experimental protocol for the pilot, including motivation for the design, selection of pilot participants, and a description of how the pilot participants interact with the electronic reporting system	Design Document
Detailed architecture of the electronic	System Implementation

Scope	Title
reporting system	
Results of internal tests of the Phase 1 electronic reporting system	In-house Test Results
Detailed E-mail communications with the pilot participants during Phase 1	Communications with Pilot Participants in Phase 1
Brief status of Phase 1 halfway through the use of the electronic reporting system by the pilot participants	Midpoint Evaluation for Phase 1
Technical issues encountered in Phase 1 during the use of the electronic reporting system by the pilot participants	Technical Issues in Phase 1
Conclusions drawn from Phase 1 results in the context of questions raised by the experimental protocol	Concluding Report for Phase 1
Description of the commercial off-the-shelf products used in Phase 2	Requirements Report for Phase 2
Internal test results for Phase 2	Report of Biometric In-house Test
Communications with pilot participants and a summary of the data received from the pilot participants in Phase 2	Communications with Pilot Participants in Phase 2
Preliminary results at the mid-point of Phase 2, including detailed installation results	Mid-point Evaluation Report for Phase 2
Assessment and evaluation of Phase 2 test results	Phase 2 Addendum Report: Final Evaluation / Assessment

2 Design

The following sections summarize the motivation for the design of the DMR pilot, and briefly describe the pilot's architecture and methodology.

2.1 Design Criteria of the Discharge Monitoring Report Pilot

The Discharge Monitoring Report (DMR) pilot as conducted in the State of New York was designed to explore the human factors, technical feasibility and digital signature issues involved in electronic compliance reporting using the World Wide Web. This solution was designed for DMR submitters whose DMR compliance reports would not exceed a few pages per outfall. These submitters would typically not have implemented their own information systems from

which DMR compliance data could be automatically extracted and submitted as a standard electronic data interchange (EDI) transmission. Web-based compliance reporting, as implemented in the pilot, was contemplated as an electronic reporting solution for submitters who otherwise would prepare DMR reports manually.

Since DMR compliance enforcement can involve litigation for criminal fraud, the ability to strongly bind the signer of the DMR to the content of the DMR was a key design criterion of the pilot. Therefore, from the outset, the legal requirements for Web-based submission of the DMR compliance report were seen as fundamentally different from the Web-based submission of purchase orders within electronic commerce. The pilot's design was therefore strongly influenced by the requirement to achieve a convincing digital signature that could withstand the scrutiny of a vigorous defense in a jury trial.

In addition to fulfilling the need for a strong digital signature, the pilot was designed to maximize the use of commercial off-the-shelf (COTS) software and document formats that are generally used on the Internet, in contrast to software specific to DMR reporting. In finalizing the DMR pilot's design, a natural tension emerged between the requirement for a strong digital signature, on the one hand, and the requirement to use familiar Internet software and methods, on the other.

To reduce the complexity of implementing and interpreting the DMR pilot, a specific Web browser manufacturer and version (Netscape Navigator 4.51) was selected for use by the pilot participants. For both human factors and legal reasons, Adobe's Portable Document Format (PDF) was selected as the document format for the DMR form, and Adobe's Exchange form plug-in (Version 3.01) was selected as the software used to manipulate the form within the context of the browser. Most people using the World Wide Web will ultimately have had the experience of using an Adobe PDF reader to view PDF documents within their browser. Since the DMR pilot was designed to use standard Web HTML forms for menus and help screens, and to display the DMR forms in PDF format, the design of the pilot was in the mainstream of Internet tools and techniques.

On the other hand, the need for an electronic form environment for the DMR which can operate as a plug-in within a Web browser and allow the submitter to fill in data fields and submit results required a more functional browser plug-in than the more familiar Adobe reader used to view PDF documents on the Web. It was necessary to use Adobe's electronic form application, Adobe Exchange, a software application normally sold commercially within a larger package of applications called Adobe Acrobat, although Adobe Exchange can function independently of the other Adobe Acrobat components. Unlike Adobe Reader that can be downloaded and installed automatically over the Internet, Adobe Exchange is distributed on a CD. Therefore the need for an

electronic form functionality for the DMR logically introduces an extra installation step and more complex software than most users would otherwise encounter in using PDF documents on the Web. However, the value of using the PDF document standard is retained.

Adobe PDF format was selected over and above other possible ways of representing the DMR form primarily for two reasons, one related to the legal meaning of a digital signature and the other related to human factors:

- The Adobe postscript and PDF formats have earned a reputation over time as a de facto standard for the faithful representation of document content across a variety of different computer screens and printers. From a legal perspective, a reasonable claim can be made that the DMR content in PDF format displayed by an Adobe plug-in will be visually represented to the signer in an expected way across different computer displays and platforms. Since, when a digital signature is applied, it is the electronic format (the ones and the zeroes) which is used as input to the generation of the signature (in cryptographic digital signatures) or bound to the signature (in the case of biometric digital signatures), the digital signature is only meaningful if there is a reliable correspondence between the electronic format of the document and its visual representation to the signer.
- The PDF format as rendered by an Adobe application offers a visual presentation of the electronic DMR form which is immediately recognized as nearly identical to the familiar paper DMR form. From a human factors perspective, the electronic DMR can be intuitively understood from a background of experience with a paper DMR without the visual compromises which would be introduced by standard HTML rendering. Further, the scrolling and magnification tools provided by the Adobe viewing application (Adobe Exchange) allow the electronic DMR form to be inspected in an intuitive way without the need to divide the DMR into subforms or require horizontal scrolling to view the complete form content. [A previous field test of an electronic Submonitoring Report (SMR) showed that submitters had difficulty understanding the compromises required to represent the SMR form as a standard HTML Web page.]

  The use of Adobe PDF format to represent the DMR form also facilitates the application of a digital signature, since it is technically possible to apply a digital signature to the entire contents of the DMR form by using a digital signature plug-in to the Adobe Exchange application. If, on the other hand, the DMR form is represented by a standard HTML Web form, current Web browsers do not provide sufficient access to both the form template and name-value pairs (field values) to allow third-party signing plug-ins to obtain the complete contents of the form to use as input to the cryptographic signature algorithm. With the

addition of browser programming extensions such as Java or ActiveX, it is technically possible to gain access to the DMR form content, as well as to enhance the appearance and functionality of the DMR form over a plain HTML Web form, but at the loss of the legal advantage of the Adobe PDF format related to a de facto history of faithful content representation.

One of the design goals of the DMR pilot was to test the functionality of using external hardware devices (smart cards, smart card readers and graphic tablets) as part of the application of the digital signature. At the time the DMR pilot was designed, there was the concern that software-only digital signatures may prove to be too weak to meet the legal requirements posed by the DMR. Therefore, in the Phase 1 of the DMR pilot, smart cards (plastic cards containing a microprocessor) were used to generate the private key as an input to the digital signature algorithm. The smart cards were read by an external smart card reader device that attached to the submitter's computer through a serial port and was powered by a cable to the keyboard port. In Phase 2 of the DMR pilot, an external graphics tablet was used to capture the dynamics of handwritten signatures. The graphics tablet was attached to the submitter's computer through a cable to the serial port, and was powered by a separate cable to the keyboard port.

The use of hardware devices added complexity to the DMR pilot in a number of ways. Additional steps in the DMR pilot setup procedures were needed to install the devices and the software needed to support them. Because the devices used the serial port of the submitter's computer, there were more potential complications related to interrupt conflicts with other devices installed on the submitter's computer. Also, conflicts with mouse drivers, power saving features, and computer shutdown behavior were noted. The additional software needed to interface with these devices created another software layer in the signing process which was subject to problems of compatibility with other software layers and the operating system.

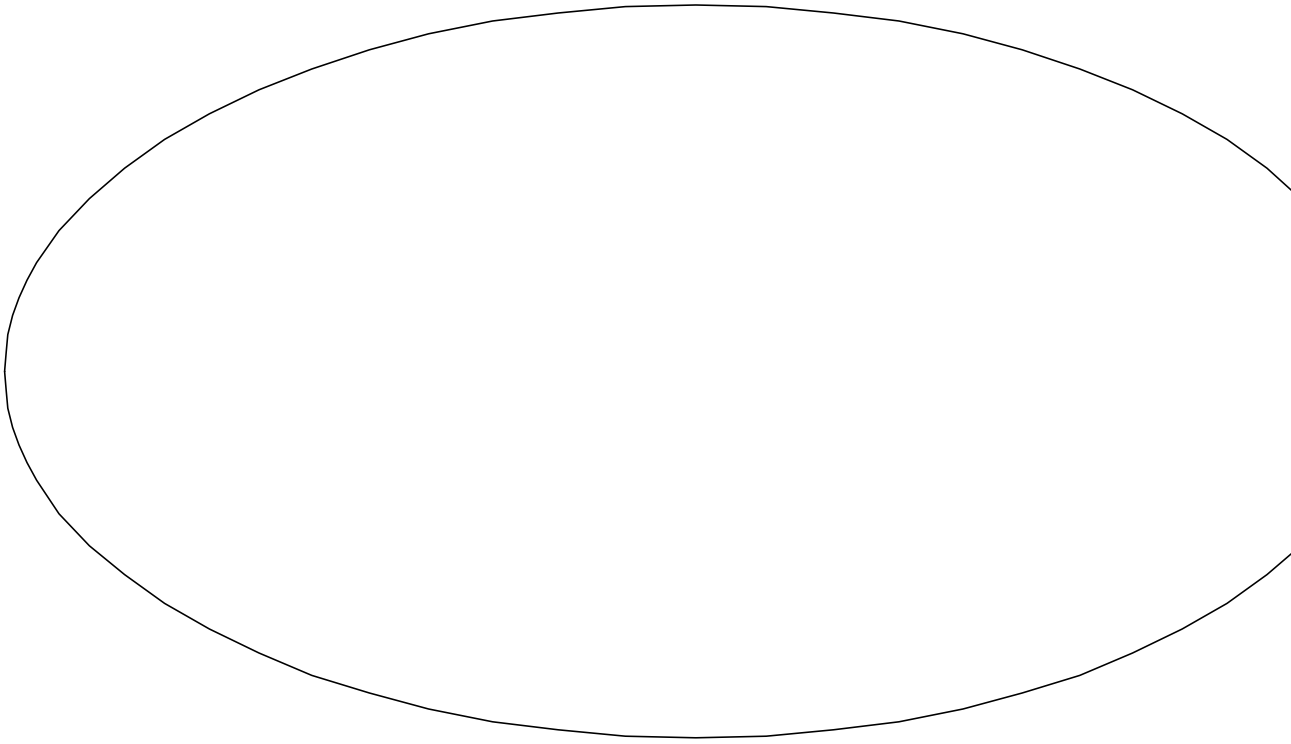
In summary, the design of the DMR pilot was derived from the following key requirements:

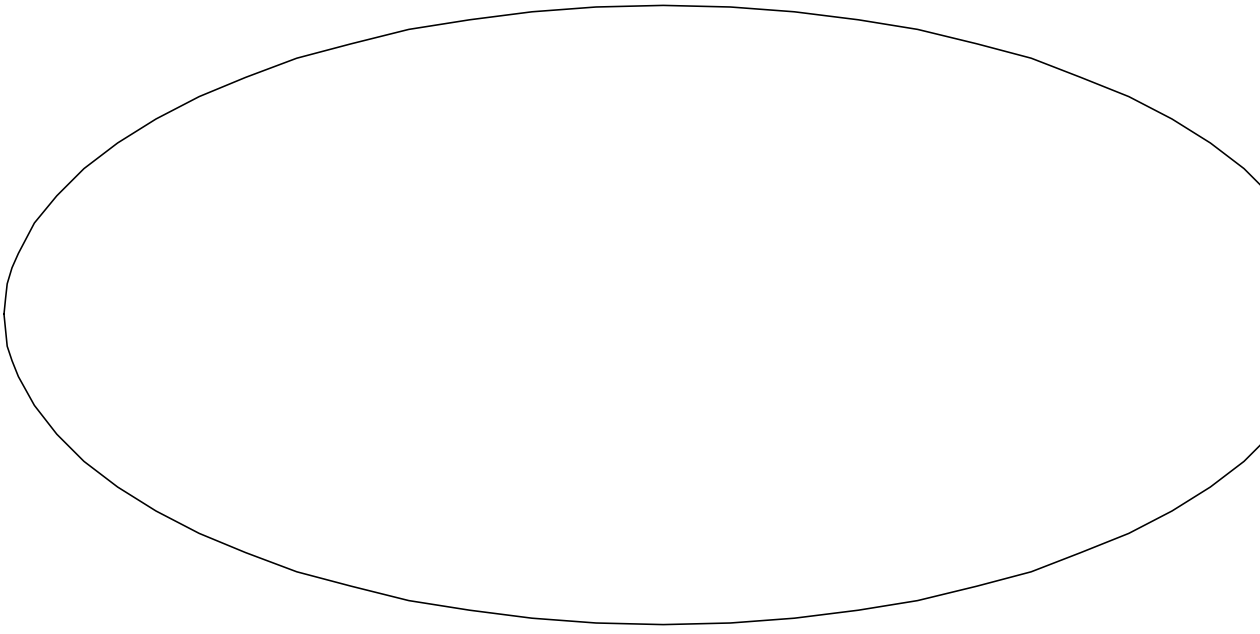
- The DMR submission process should maximize the possibility that the digital signatures applied to the electronic DMR forms will be convincing to the jury in a trial that focuses on the accountability of the signer for a false DMR submission.
- The DMR submission process should maximize the use of familiar tools and techniques of the World Wide Web.

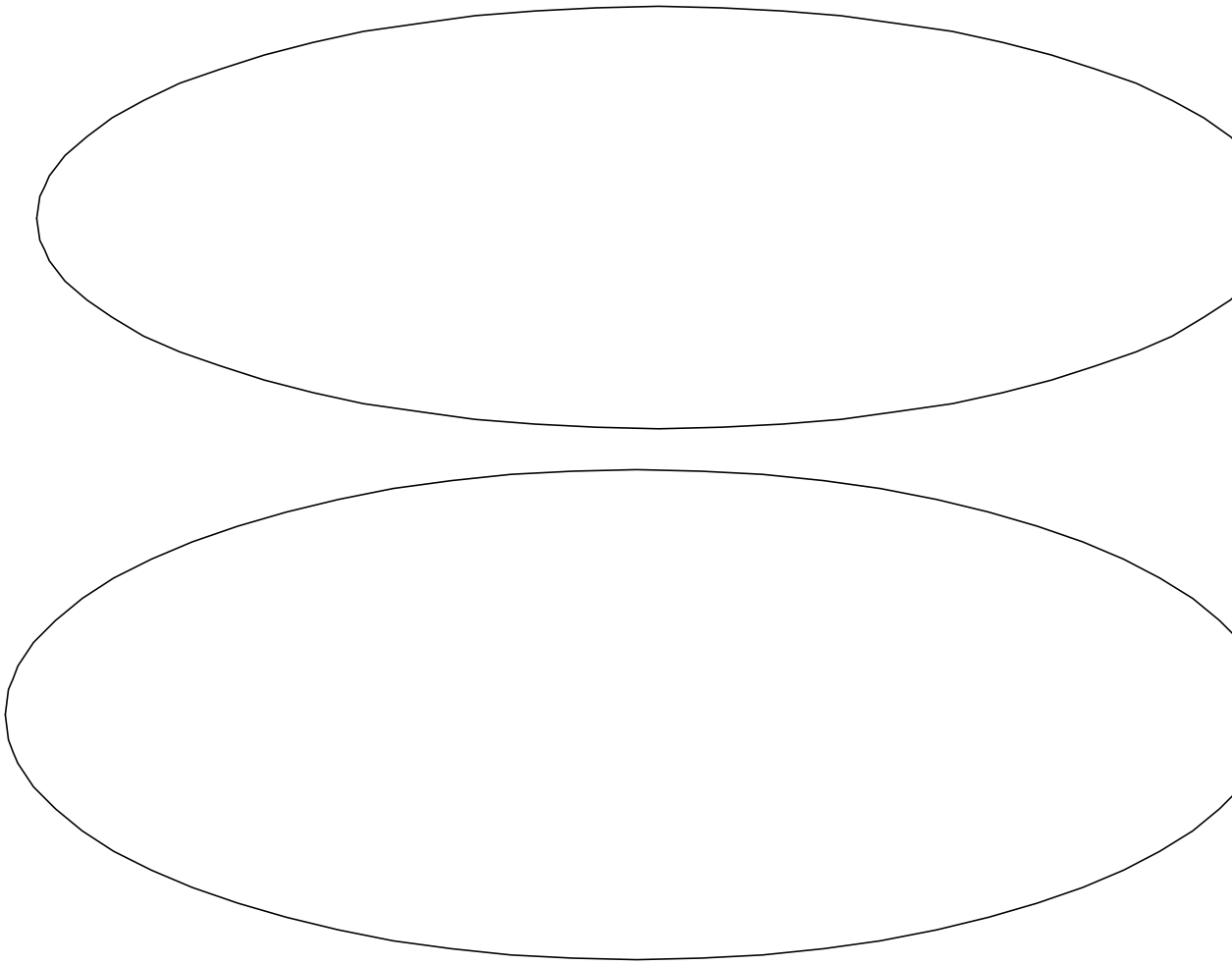
- The DMR submission process is intuitive and offers advantages over the manual preparation of paper DMR forms.
- The DMR submission process should maintain sufficient reliability in the chain-of-custody and in the integrity of the data to assure that the data contained in the signed DMR forms are stored without alteration in a receiving database and transmitted to the compliance authority (the New York State Department of Environmental Conservation).

These design criteria led to an implementation of electronic DMR submission which was necessarily more complex than the routine use of Web forms in e-commerce, but which also demonstrated methods for achieving a digital signature with a strong claim to legal significance.

6.1 Design and Architectural Overview

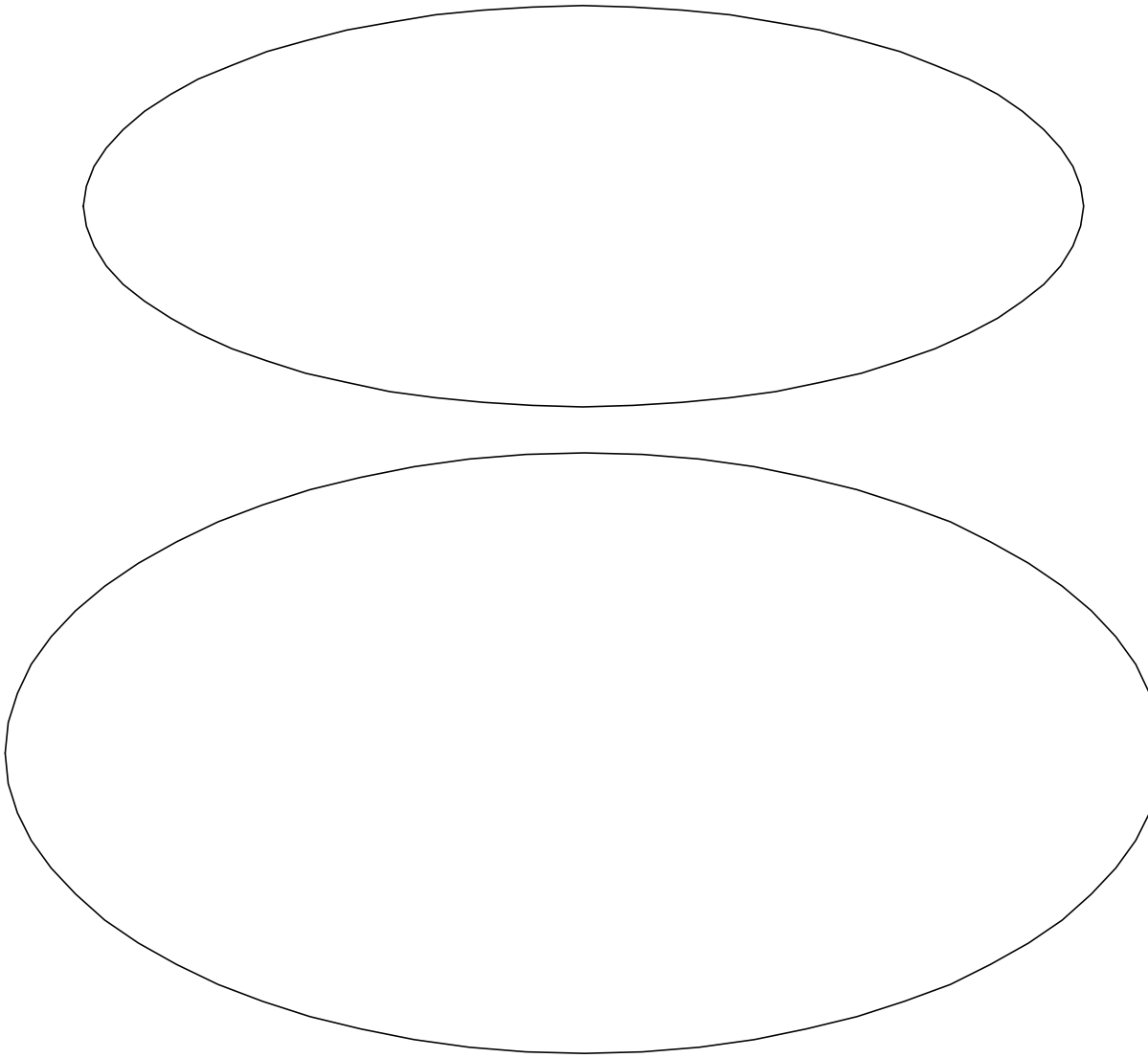






The New York DMR pilot was designed as a complete compliance reporting system, with a fully functional public key infrastructure (PKI) and a complete data flow among the submitter, receiving site, compliance authority, certificate authority, and EPA's Permit Compliance System (PCS) as shown in Figure 1:

Figure 1



The flow of submitted DMR data begins with the submitting organization. The submitter completes an electronic DMR form, digitally signs the form, and then submits the form data to the receiving Web site. The receiving Web site stores the submitted

data in a database, verifies the digital signature, and then transmits the submitted data to the compliance organization (the New York State Department of Environmental Conservation). The compliance organization verifies the data, which is then available for entry into EPA's Permit Compliance System.

The flow of facility and parameter information, required to provide each submitter with the correct selection of form templates containing prepopulated data, begins with EPA's Permit Compliance System. The compliance organization, the New York State Department of Environmental Conservation, then adds their data elements based on the permit established with the submitting organization. These data are transmitted from the compliance organization to the receiving Web site for use in establishing Web-based menus of available pre-populated DMR forms by permit number, reporting period, and discharge number.

In Phase 1 of the DMR pilot, the flow of identity information, required for the initial setup enabling subsequent digital signatures, begins with the submitting organization. The submitting organization sends identity information (e.g., signer's name, organizational affiliation, E-mail address) directly to the Certificate Authority using a Web form provided by the Certificate Authority. The compliance organization, the New York State Department of Environmental Conservation, acting as the Local Registration Authority, uses a Web form over an Internet connection secured by client-authenticated Secure Sockets Layer to review and approve the submitted identity data based on a manual comparison with permit records.

If approved, the signer receives an E-mail message sent from the Certificate Authority containing an access code. The signer then uses pre-installed software to generate a public-private cryptographic key pair and then sends the public key to the Certificate Authority using a Web form enhanced with automatically downloaded software components. In the DMR pilot, cryptographic keys were generated in hardware using a microprocessor on a plastic card (a smart card). To complete the step of sending the signer's public key to the Certificate Authority, the signer must enter the access code in the Web form. The signer then receives a copy of the certificate containing the signer's identity information and public key. The Certificate Authority also stores the signer's certificate in the Certificate Authority's database.

Once the setup, or certificate request and registration process, has been completed, the signer signs subsequent DMRs by regenerating the signer's private key. The receiving Web site verifies the signer's signature with the public key contained in the signer's certificate as stored in the Certificate Authority's database. At any time, the compliance organization (the New York State Department of Environmental Conservation), acting as the Local Registration Authority, can revoke the certificate by using a Web form provided by the Certificate Authority. The revoked certificate appears in a Certificate Revocation List available to the receiving Web site.

In Phase 2 of the DMR pilot, DMR forms were signed using the signature dynamics data generated by the signer's handwritten biometric signature applied with a plastic stylus to a graphics tablet. The signature dynamics data were bound to the contents of the DMR form by symmetric key cryptography. In order to verify these biometric digital signatures, signers completed a Web enrollment form in which the signer submitted a minimum of five signature samples to the receiving Web site. A pattern recognition program running at the receiving Web site was used to verify that the biometric signatures applied to subsequent DMR submissions matched the enrolled signatures within a pre-selected level-of-confidence score. Phase 2 relied on the previous preparation of Phase 1 to bind the identify of the signer to the set of enrolled biometric signatures, and did not attempt to establish a full-featured independent security model tailored uniquely to biometric signatures.

6.2 Brief Summary of DMR Pilot Methodology

Seven pilot participants representing public and commercial organizations with facilities in the State of New York were selected by the New York State Department of Environmental Conservation based on the following criteria:

- The pilot participant responded favorably to an invitation from the New York State Department of Environmental Conservation to join the DMR pilot.
- The pilot participant's facility held a current permit in New York State to discharge to an open body of water.
- The pilot participant's DMR did not exceed three pages per discharge number (outfall).

- The pilot participant's facility was located no more than a half-day driving distance from Albany, New York.
- The pilot participant agreed to commit the necessary time to complete the pilot.
- The pilot participant's facility agreed to provide computing equipment and routine technical support.

The pilot participants attended a one-day introductory briefing and training session hosted by the New York State Department of Environmental Conservation (NYS DEC) in Albany, New York. After a period of in-house testing of the pilot hardware and software configurations, a representative of InDyne, Inc. (IDI) met with the NYS DEC staff who had been assigned to work with the pilot in Albany, New York. The purpose of this meeting was to assist with the installation of the pilot hardware and software components at NYS DEC, including the hardware and software that NYS DEC would use to access the Certificate Authority during Phase 1. At the beginning of Phase 1, a representative from IDI joined the NYS DEC staff in visiting each pilot facility to observe each pilot participant install the pilot hardware and software components on the pilot participant's computer based on written directions customized for the pilot. The pilot participant was encouraged to perform the installation based on written directions. IDI and NYS DEC representatives provided help if the pilot participant could not successfully complete a step in the installation process.

Pilot participants were asked to contact the Certificate Authority's Web site and fill out an enrollment form with basic identity information (e.g., name, facility, E-mail address). In many cases, this step was completed while the IDI and NYS DEC representatives were present at the pilot participant's facility. Pilot participants were then asked to wait for an E-mail message from the Certificate Authority containing an access code that could be used to complete the certificate registration process. The pilot participant then subsequently attempted to complete the registration process by using the smart card to generate a public-private cryptographic key pair while providing the access code to the software interface used for certificate registration. After a testing and experimentation period of approximately two weeks, pilot participants were asked to electronically submit, over a two-month period, six DMRs containing the same data as previously submitted on official paper DMRs for the previous six months. Teleconferences were held with the pilot participants to discuss problems and observations.

During Phase 1 of the pilot, NYS DEC performed the function of a Local Registration Authority (LRA) using a series of Web forms provided by the Certificate Authority. Access to the LRA administrator's Web forms was protected by a client-authenticated Secure Sockets Layer (SSL) connection. The cryptographic key for client authentication was generated by a smart card in

communication with the LRA administrator's computer. NYS DEC also verified submitted DMR data by comparing the electronic submission with previous paper DMR submissions.

At the beginning of Phase 2, a team consisting of representatives of NYS DEC accompanied by a representative from EPA Headquarters visited each pilot participant's facility to assist with the installation of the Phase 2 hardware and software components. As in Phase 1, each pilot participant was encouraged to perform the installation steps based on written instructions, with NYS DEC providing additional assistance if the pilot participant could not complete an installation step. After completing the installation, pilot participants were asked to enroll their handwritten biometric signatures by signing an enrollment Web form five times using a plastic stylus and a graphics tablet. As in Phase 1, pilot participants were asked to electronically submit and sign DMRs with data corresponding to six months of historical paper DMRs.

13 Results

The following subsections summarize the principal results of the DMR pilot. Because the pilot involved a number of activities, components and tests, the following discussion will attempt to dissect a large body of data from a variety of viewpoints.

13.1 Anticipated vs. Unanticipated Risks

A number of risks were anticipated for the DMR pilot, including:

- The Adobe Exchange electronic form may exhibit different behavior when used with different browsers.
- The Adobe Exchange electronic form may have limitations in data capacity, ability to be configured to fully support the DMR form, or in the ability to pass large amounts of data through the browser to the Web site.
- The digital signature plug-ins, both cryptographic and biometric, may have limitations in their ability to sign the complete contents of the form and pass signatures back to the Web site.
- The pilot participants may have difficulty in installing the pilot hardware and software components from written instructions.
- The variety of existing hardware and software environments provided by the pilot participants may introduce compatibility problems with the new hardware and software components installed for the pilot.

- The pilot participants and the New York State Department of Environmental Conservation may have difficulty understanding and executing the steps needed to set up a complete public key infrastructure (PKI) needed to sign and verify cryptographic digital signatures.
- The pilot participants may have difficulty accessing the Certificate Authority's Web server and the receiving Web site established for the pilot due to a variety of existing methods used to connect to the Internet.
- The pilot participants may have difficulty installing and using the hardware devices (the smart card and graphics tablet) used in the signing process.
- The New York State Department of Environmental Conservation may have difficulty processing and verifying the submitted DMR data received at the pilot Web site.

The actual pilot results were surprising to the extent that many of the high-level anticipated risks proved not to materialize in the way, or in the degree, which were expected. However, a large number of more detailed unanticipated technical risks emerged which proved to be significant.

For example, the process of establishing and implementing a complete public key infrastructure (PKI) for the DMR pilot was easier than anticipated, and functioned well in the sense that the pilot participants could follow instructions to enroll their identity information using a Web site, and the New York State Department of Environmental Conservation could approve new enrollments using a set of Web forms provided by the Certificate Authority. Unanticipated problems in the use of the PKI established for the pilot included more technical details such as:

- Three of the pilot participants could not initially access the Certificate Authority's server to complete their certificate registrations using the client software initially provided for this purpose by the Certificate Authority due to the network firewall implemented by the pilot participant's facility. The Certificate Authority provided a Web-based certificate registration process to solve this problem.
- Certificate registrations could sometimes not be completed due to network congestion at the Certificate Authority's site, or due to technical problems with the cryptographic services in the operating system of the pilot participant's computer, or, less frequently, due to technical problems with the Certificate Authority's database.

The pilot participants were able to follow instructions related to signing DMR forms using smart cards, but did not seem to have an intuitive grasp of the cryptographic signature mechanism as evidenced by several pilot participants who attempted to add information to the DMR form after completing their cryptographic signature.

Anticipated risks related to the ability of the New York State Department of Environmental Conservation (NYS DEC) to exchange data with the receiving Web site were in general not realized in the pilot. NYS DEC successfully transmitted the information to the receiving Web site necessary to establish the selection menus and pre-populate the DMR forms with facility and parameter information. NYS DEC also successfully received submitted data from the Web site, as well as verified the submitted data stored at the Web site by viewing the completed DMR forms with Web browsers.

In the DMR pilot, some anticipated risks related to the variety of hardware, operating systems and software used by the pilot participants were realized. Some specific examples of these realized risks included:

- Two pilot participants had computers with compact disk (CD) drives which could not read the CD-ROM media used to distribute some of the pilot software.
- One pilot participant used a digital camera connected to the only available serial port on his computer. The substitution of a smart card reader for the digital camera forced changes in the configuration of the supporting software for the digital camera.
- Several pilot participants experienced problems with shutdown or alterations in the behavior of the power saving features on their computers when the smart card reader was installed. An update in the operating system's smart card driver library was needed to resolve most of these problems.
- The installation of software supporting the graphics tablet used to capture biometric signatures behaved differently on different operating systems. A version update of this software was necessary to resolve these installation differences.
- One pilot participant used an internal communications card that generated an interrupt conflict with the serial port used for the smart card reader. It was necessary to change the serial port interrupt to resolve the conflict.

Differences in the behavior of the Adobe Exchange Version 3.01 application when used with Internet Explorer 4.01 and Netscape Navigator 4.51 were observed during in-house tests. These differences were more pronounced and dramatic than anticipated, including:

- Opening new DMR forms with Adobe Exchange within Internet Explorer launched a new window and a new instance of Adobe Exchange with each DMR form selected, whereas a single window was reused and single instance of Adobe Exchange was launched within the context of Netscape Navigator.

- The use of secure sockets layer (SSL) appeared to require significantly more memory overhead within Netscape Navigator compared with Internet Explorer, limiting the number of DMR pages which could be loaded with pre-populated data received from the Web site when SSL was used with Netscape Navigator.

31.1 Results related to PKI

The public key infrastructure (PKI) implemented for the DMR pilot demonstrated that certificates could be issued and managed within a small-scale, self-contained compliance program such that:

- The compliance authority (the New York State Department of Environmental Conservation), acting as the Local Registration Authority, could approve certificate registrations and manage certificates using a browser interface to the Certificate Authority. This activity used a minimum of administrative overhead and primarily required the New York State Department of Environmental Conservation to compare the identity information submitted by the pilot participants in their certificate requests with previous paper records describing the participants and their permits.
- The design of the PKI suggested a logical path of scalability to larger number of participants by increasing the number of people acting on behalf of the Local Registration Authority, and to multiple compliance programs by adding Local Registration Authorities as needed.

The difficulties that surfaced using the PKI within the DMR pilot resulted from the following types of technical challenges:

- The Certificate Authority server, located in Wisconsin and accessed over the Internet, was sometimes not available due to network congestion or server maintenance.
- E-mail messages, sent from the Certificate Authority to the individual requesting a certificate, were used to deliver a one-time access code required to complete the certificate registration. The E-mail gateways needed to successfully complete the delivery of this E-mail message were not always operational.
- To complete the registration of the certificate, the pilot participant must generate a public cryptographic key using both hardware (smart card) and software components, including cryptographic components contained within the operating system of the participant's computer. The ability to generate a public-private key pair, and supply the public key to the Certificate Authority, depends on a complex and multi-layered set of interactions on the participant's computer that introduce multiple potential

failure modes. In the DMR pilot, the following types of problems related to completing a certificate registration were observed:

- The smart card was not initialized prior to being used for creating a public-private key pair.
- The behavior of the smart card depended upon the point in the sequence of steps the smart card was inserted in the smart card reader.
- The pilot participant forgot the personal identification code needed to use the smart card.
- The cryptographic components of the operating system of the participant's computer became corrupted and required either a re-registration attempt or a re-install of the cryptographic components.
- A database record in the Certificate Authority's server containing identity information became corrupted and blocked the completion of the certificate registration.
- A network firewall used by the participant's organization blocked the network protocols required to complete the registration.

In summary, the PKI used in the DMR pilot was easy to install and administer, and therefore demonstrated the feasibility of using a PKI to support electronic compliance submissions. The number of possible failure points in the generation of cryptographic keys on the participants' computers suggested that the support issues involved in maintaining a PKI on a larger scale would center primarily in the effort needed to maintain the health of cryptographic components on the pilot participant's computer, where these components are both multi-layered and multi-vendor, and involve the participation of cryptographic components of the operating system.

Within the pilot, problems related to network connectivity of the pilot participant's computer with the Certificate Authority's server, were mostly resolved as the result of experience gained as the pilot progressed. For example, the problem of reaching the Certificate Authority's server through the pilot participant's firewall was solved by creating a browser-based registration process.

42.1 Reactions of Pilot Participants

On the whole, the pilot participants were gracious and positive about their involvement with the DMR pilot, and expressed an interest in the approaches and technologies that the pilot introduced. Two pilot participants withdrew from active participation in the pilot due to lack of time and internal technical and management support to work through technical problems encountered in the pilot. In one case, an initial problem reaching the Certificate Authority

server through the participant's corporate firewall prevented an initial successful result in completing the certificate registration process. Subsequently, a major network reconfiguration within the pilot participant's organization introduced a competing priority for the organization's limited internal technical support resources. In another case, after resolving problems related to installing the smart card reader on the same serial port previously used for connecting a digital camera, the corruption of the cryptographic component of the operating system on the pilot participant's computer prevented the pilot participant from successfully completing the certificate registration process. This problem could not be easily resolved by remote technical support, and the pilot participant withdrew because, as stated by the participant, the participant's organization did not provide sufficient release time from other duties and responsibilities to work through this issue.

The remaining pilot participants completed the pilot, responding to various technical difficulties with grace and patience. For any given pilot participant, these difficulties included one or more of the following challenges:

- The pilot participant's CD drive would not read some of the rewritable distribution CDs containing the pilot software.
- The smart card reader could not be recognized, or produced intermittent side effects, due to a serial port interrupt conflict with another previously installed device.
- The operating system's smart card driver library prevented a normal system shutdown, or interfered with the power management features of the participant's computer.
- The pilot participant's computer would "freeze" if the smart card was inserted after the browser was launched.
- The pilot participant could not access the Certificate Authority server through the participant's firewall.
- The pilot participant experienced a server-side time-out before the participant could successfully submit a DMR form.
- The loading of pre-populated data into the DMR form did not complete successfully.
- The behavior of the pilot software during installation on the pilot participant's computer deviated from written instructions previously developed and tested on in-house computers.
- The Internet Service Provider used by the pilot participant did not provide reliable service.

- The smart card permanently self-destructed after the pilot participant forgot the personal identification number (PIN) needed to activate it, and typed the wrong (PIN) more than three times.
- The signature name and date were not saved with the DMR form data as expected.
- The DMR comment form could not be successfully signed.
- The DMR form could not be saved due to the failure of database update at the server.
- The electronic Adobe DMR form would not load the pre-populated data the first time it was launched after a memory-intensive had been used on the pilot participant's computer.
- The electronic Adobe DMR form contained fields with format and verification rules that were less flexible and more strictly enforced than the same fields in paper DMRs.
- The Adobe DMR form contained parameter rows sorted in a different order than the pilot participants had experienced with paper DMRs.
- Data entered into the Adobe DMR form fields were rendered in a font that was smaller than could be comfortably read in the default full-screen magnification of the form on the screen.
- The default vertical behavior of the tab key when moving from field to field in the Adobe DMR form differed from horizontal behavior expected by the pilot participant.
- The digital signature plug-in changed the screen colors of the DMR form if certain screen resolutions were set on the pilot participant's computer.
- The screen cursor disappeared within the digital signature dialog box.
- The pilot participant's enrollment of a sample of biometric handwritten signatures failed.

As a broad generalization, during Phase 1 of the DMR pilot the majority of the technical challenges occurred during the installation of the hardware and software, the registration of the certificate, and the initial attempts to submit and sign DMR forms. Most of these technical issues were subsequently resolved so that, after a successful setup had been achieved, all of the pilot participants, with the exception of the two participants who withdrew from the pilot, were able to submit and sign electronic DMRs with data corresponding to six months of historical DMRs by the conclusion of Phase 1.

It was immediately apparent that the pilot participants intuitively understood the meaning and format of the electronic Adobe DMR form, as the pilot

participant's began using the form as soon as it was introduced without asking questions related to how to fill it out. With the exception of some of the difficulties in working with the form listed above, the pilot participants found the form easy to understand and complete. A telecon with the pilot participants at the end of Phase 1 elicited general comments similar to, "Once I got set up, filling out each DMR submission took less than ten minutes." In general, the pilot participants thought that the Web-based submission of DMRs was "the way to go" in the future.

In Phase 2 of the DMR pilot, the participants were asked to sign their DMR submissions with a biometric handwritten signature captured with a plastic stylus and graphics tablet. Although most of the pilot participants experienced technical difficulty in completing the enrollment of their handwritten signatures, some of the participants made the comment that they found the biometric signature more meaningful, intuitive and easier to understand than the cryptographic digital signature method used in Phase 1. The pilot participants took an interest in the graphics tablets during the Phase 2 installation and seemed to enjoy the familiarity of signing their name with the plastic stylus. One of the pilot participants illustrated this feeling quite graphically by holding up the smart card reader used in Phase 1 with one hand while holding the graphics tablet used in Phase 2 in the other. With what appeared to be a note of appreciation for the graphics tablet, the participant stated, "Now this [looking at the graphics tablet] makes a lot more sense than this [looking scornfully at the smart card reader].

63.1 Fundamental vs. Transient Technical Issues

Of the various technical issues encountered in the DMR pilot, some of these issues were dependent upon the specific versions of the software used or represented minor technical problems which either were resolved within the duration of the pilot, or could be resolved with more time and resources. Other issues were more fundamental, in that they would likely apply in future implementations of electronic reporting with a similar design, even if the specific instances of the reporting system's architecture were updated or modified. Some issues could be categorized as theoretically solvable with time and effort, but are nevertheless representative of considerations which would need to be addressed in any electronic reporting system of production scope.

During the DMR pilot certain technical problems could be attributed to the maturity of the software, and could reasonably be expected to be resolved in later releases of these products. For example, the proprietary software components supplied by the smart card manufacturer (Gemplus) were in their first production version release. The smart card driver library and cryptographic components supplied by the operating system (Windows 95, 98 and NT) were also early releases. In the case of Windows 95 and NT, the

cryptographic components were added as recent updates to these operating systems, installed as an Internet Explorer browser update. Problems related to the behavior of the smart card drivers and their interaction with the operating system's cryptographic components on the pilot participants' computers (e.g., freezes or crashes if the smart card was inserted after the browser was launched, or interference with shutdown and power management) were attributed to defects in these early software releases, both in the basic components of the operating system and in the third-party add-ons.

Similarly, both the cryptographic and biometric signature plug-ins employed in the pilot were early releases of these products. Minor technical problems such as changes in the display characteristics of the form when the user interface of the plug-in was launched and then closed on computers with certain screen resolutions, or the disappearance of the cursor if a pre-existing customized cursor setting was used, represent technical challenges which could reasonably be expected to be overcome by updates in these products. An internal buffer overflow problem in the server-side application server by Haht Software was resolved by updating to a later build of this software component. Initial problems installing the CalComp graphics tablet on some computers were overcome by upgrading to a later software release.

During the course of the pilot, a number of technical challenges emerged which suggested that many of the software components needed to implement an open-architecture, Web-based electronic form with faithful content representation, on-line interaction with a Web site and strong digital signatures are still in the early stages of development. On the other hand, many of these challenges were overcome by obtaining updates or patches from the manufacturers of these components during relatively short duration of the DMR pilot. This experience suggested that the implementation of an electronic reporting system could be expected to reveal a set of detailed technical problems as the scope of the implementation increased beyond small-scale or in-house tests to a wider community of participants. The ability to resolve many of these technical issues also suggested that these issues could be overcome with good cooperation from the software manufacturers.

Other technical challenges observed in the DMR pilot could be attributed to configuration settings that needed to be fine-tuned based on experience with actual pilot operation. These included buffer size settings, browser cryptographic settings, database and application server time-outs, biometric signature accept/reject thresholds, etc. Like the minor technical problems encountered with early versions of the software components, these configuration settings represent considerations with short-term significance, in that they could reasonably be optimized given sufficient experience with the detailed performance characteristics of any given electronic reporting system.

On the other hand, other technical issues observed during the DMR pilot pointed to more fundamental, longer-term considerations that represent fundamental trade-offs or design tensions. These issues transcend the examples of more transient, short-term technical challenges like those discussed above. Examples of these longer-term, more fundamental considerations include:

- The modular, open-architecture design of the DMR pilot allowed the strengths of familiar software products, such as Netscape browsers and Adobe Exchange electronic forms, to interact with each other and with specialized digital signature products through standard interfaces. This open architecture design allows a given functionality of the overall electronic reporting system to be provided by the best-supported product available to meet this component functionality. It also reduces the risk of obsolescence by allowing any specific component of the reporting system to be replaced without replacing all of the components. On the other hand, a multi-vendor design introduces the necessity of achieving and maintaining functional compatibility among all of the interacting system components across time and separate version updates, recognizing that the operating system type and version, and the total configuration of the participant's computer, including the other software products and devices which may have been previously installed, must be considered as part of the total integration for which internal compatibility must be maintained.

- When using commercial off-the-shelf (COTS) products to meet the specific functional requirements of the components of an integrated electronic reporting system, it is possible that the use of these COTS components for electronic reporting will make unusual demands on one or more of these components beyond the normal use of these products individually. For example, in the DMR pilot, memory limitations of the browser and the application server were exceeded due to the special demands imposed on these products resulting from the need to transmit large amounts of data from the server to the participant to pre-populate multiple pages of a DMR form, and also to send the information generated by the biometric signature from the participant to the server.

- The use of familiar, mainstream COTS products for electronic reporting has the advantage of reducing the special training, support and user acceptance issues raised by a more proprietary alternative. However, the need to integrate with other components of the reporting system that may be specific to the DMR form or to security requirements may require that new features of these familiar COTS products be used, or that the user become more familiar with the configuration settings of these products. For example, in the DMR pilot, the pilot participants needed to become familiar with the caching and security settings of their browsers in a way that they may not have needed to know for general Internet browsing.

- To the degree that the security and signature authentication requirements of electronic compliance reporting are determined to exceed that of electronic commerce as it is popularly implemented in familiar COTS products, the electronic reporting system must introduce some combination of new security procedures, software and/or devices that introduce additional complexities and potential points of failure. To the degree that the electronic reporting system adds procedures or components not normally used by the submitter outside of the electronic reporting requirement, the reporting system adds installation, maintenance, compatibility and technical support challenges beyond those normally encountered by the end user when using these COTS products for other more general purposes.
- Specific characteristics of the participant's computing environment, such as the method of connecting to the Internet, the presence of firewalls and load-balancing routers that affect network traffic from the participant's computer to and from the external Internet, and the presence and configuration of network cards, modems, digital cameras, and other peripheral devices, as well as the specific version and configuration of the operating system and installed software, and the possible presence of viruses, corrupted files, and other factors affecting the health of the participant's computing environment, all contribute to the potential for a high degree of individual variation in the behavior of an electronic reporting system as it is used by any given participant with a specific end-user computing environment.

68.1 Results Related to Digital Signatures

In the DMR pilot, Phase 1 employed cryptographic digital signatures in which a smart card generated the private cryptographic key. In Phase 2, a biometric handwritten digital signature was used. In the DMR pilot, the cryptographic digital signatures used in Phase 1 were more successfully implemented than biometric digital signatures used in Phase 2, in that more participants were successful in submitting DMR forms signed with cryptographic digital signatures. On the other hand, the pilot participants seemed to more intuitively understand the biometric signature method.

As a broad generalization, the failure modes of the cryptographic digital signature method observed in the pilot were attributable to user error, or to the fragility of a complex chain of interacting hardware and software components from multiple vendors, including the supplier of the operating system. Failure modes observed with the biometric signature method were primarily due to problems inherent with biometric signatures, such as the challenge of creating an acceptable set of enrollment signatures, or to technical problems related to the storage and transmission of the much larger volume of biometric signature data by the Adobe form, Netscape browser, and HAHTsite application server as compared with cryptographic signatures.

Results specific to these two signature methods are summarized in separate sections below.

68.1.1 Cryptographic Digital Signature Results

In addition to the components and conditions required for the successful registration of certificates within the PKI infrastructure established for the DMR pilot, the cryptographic digital signature mechanism used in Phase 1 of the DMR pilot depended on the operation of multiple components on the signer's computer, including:

- the smart card,
- the smart card reader,
- the serial communications from the smart card reader to the signer's computer,
- the proprietary software drivers supplied by the manufacturer of the smart card reader (Gemplus),
- the smart card driver library supplied by the operating system (Microsoft),
- utility programs supplied by the manufacturer of the smart card reader,
- the Cryptographic Service Provider supplied by the manufacturer of the smart card (Gemplus),
- the cryptographic application programming interface supplied by the operating system,
- other cryptographic components of the operating system, including access to stored certificates,
- the Web browser with its internal buffers and communication mechanisms (Netscape),
- the electronic form plug-in with its internal buffers and communication mechanisms (Adobe Exchange),
- the application programming interface supplied by the electronic form for use by form plug-ins,
- the digital signature plug-in (E-Lock Technologies' Assured Transactions)
- operating system function calls for screen display, cursor movement, process control and communication.

In addition to these components on the signer's computer, and the necessary Internet communications, the following components were required at the receiving Web site:

- a server operating system (Microsoft),
- a Hypertext Transfer Protocol server (Microsoft),
- an application server (HAHTsite),
- a database server (Microsoft),
- a digital signature verification program (E-Lock Technologies).

In addition to the technical challenges related to the initial certificate registration process described in an earlier section on the use of the PKI infrastructure, the following technical problems were encountered by one or more of the pilot participants when applying cryptographic digital signatures in the DMR pilot:

- In the first version of the digital signature plug-in, the digital signature was encoded in Base64 format and stored in a hidden field of the electronic form. The representation of some digital signatures with Base64 encoding produced characters (line feed and carriage return) which were not processed correctly by the electronic form plug-in (Adobe Exchange) when stored in hidden fields of the electronic form. This caused a memory overrun with the electronic form and caused the participant's computer to lock up or crash after the digital signature was executed. This problem was corrected in a new release of the digital signature plug-in.
- With particular screen resolution and custom cursor settings on the participant's computer, the digital signature plug-in would change the color of the electronic form display or fail to display a screen cursor within the digital signature dialog box.
- A high-level cryptographic application programming interface supplied by the operating system and used by the digital signature plug-in failed to release allocated memory after it was no longer needed, preventing the digital signature from succeeding when used beyond the first few times. This problem was resolved by using a low-level cryptographic application programming interface which did not exhibit this behavior.
- The cryptographic components of the operating system responsible for storing and recognizing the certificate became corrupted for an unknown reason and required the re-installation of these components.
- The presence of the smart card and smart card reader interfered with the normal shutdown or power saving features of the participant's computer. These problems were mitigated by upgrading the smart card driver library supplied by the operating system.
- The participant's computer locked up or crashed if the smart card was inserted into the smart card reader after the browser was launched. This

problem was mitigated by inserting the smart card prior to launching the browser.

- The installation of a smart card reader on the serial port of the pilot participant's computer created an interrupt conflict with a previously-installed device that used the same interrupt (e.g., an internal serial communications card).

The following user errors by one or more pilot participants prevented the successful application of a cryptographic digital signature until these errors were corrected:

- The pilot participant forgot the personal identification number (PIN) needed to activate the smart card, and then disabled the smart card by entering an incorrect PIN three consecutive times.
- The pilot participant changed the content of the DMR form after applying the digital signature, thus causing the digital signature to be rejected at the receiving Web site because the DMR form data had been altered after signing. These alterations were due to the addition of a date and typed signer's name after the digital signature had been applied. This sequence of events would be intuitive for a paper signature, but this result demonstrated that the pilot participants did not understand the mechanism by which a digital signature freezes the content of the signed form when the signature is applied.

Eventually all of the participants who remained active in the DMR pilot were able to successfully sign DMR forms with cryptographic signatures. Once the digital signature mechanism was successfully established on a given participant's computer, and once the digital signature procedures were resolved, the application of signatures for the remaining test set of DMR form submissions was routine.

96.0.1 Biometric Digital Signature Results

The type of biometric digital signature used in Phase 2 of the DMR pilot is a handwritten biometric signature in which over ninety parameters of signature dynamics data related to the physics of executing a handwritten signature using a plastic stylus on a graphics tablet (e.g., acceleration, pressure, wobble, etc) are used to create a packet of information known as the biometric signature. These raw signature dynamics data are detected by the graphics tablet and transmitted to the signer's computer. A biometric digital signature plug-in (supplied by PenOp) to the Adobe Exchange electronic form then binds these signature dynamics data with a symmetric cryptographic key to the contents of the DMR form. These biometric signature data are stored in hidden fields of the

Adobe Exchange form and transmitted to the receiving Web site with the submitted DMR data.

The handwritten biometric signature mechanism used in Phase 2 of the DMR pilot was less complex than the cryptographic signature mechanism used in Phase 1 in the following two ways:

- The application of a biometric signature lacks the involvement of cryptographic components supplied by the operating system.
- The application of a biometric signature does not require a PKI infrastructure (although the binding of the biometric signature to the contents of the DMR form using asymmetric, public-private cryptographic key pairs managed within a PKI is an option for added security and strength of authentication).

The biometric signature proved technically more difficult to implement for the following reasons:

- The size of the digital representation of the biometric signature is much larger than the size of a cryptographic digital signature, and this size varies from signer to signer. In the DMR pilot configuration, the larger amount of information associated with a biometric signature overflowed internal buffers within the application server when submitted DMR data containing the biometric signature was received by the server at the pilot's Web site.
- The verification of the biometric signature at the server required that the submitted form data and the biometric signature be loaded into an instance of the electronic form application (Adobe Exchange) running on the server at the receiving Web site. The biometric signature verification program (supplied by PenOp) then ran as a plug-in to the Adobe Exchange program on the server. The architecture for verifying biometric signatures on the server required a separate computer at the receiving Web site to load Adobe Exchange and perform the verification, as well as added transaction controls to couple the biometric signature verification process to the application server.

In the DMR pilot, the participants were asked to enroll a set of five biometric handwritten signature samples, which is the minimum number of signatures that the PenOp signature enrollment program requires to complete an enrollment. However, if the PenOp enrollment program detects too great a variation among the signature samples, more signature samples are required to achieve a successful enrollment. The ability to complete a successful enrollment was demonstrated to be person-dependent in the DMR pilot, even if the enrollments were attempted on the same computer.

Although several successful biometric signature enrollments were achieved during in-house tests and within the New York State Department of

Environmental Conservation, only one pilot participant succeeded in successfully enrolling a set of biometric signatures. This same pilot participant was also successful in signing a DMR form with a biometric signature, and this signature was automatically verified at the receiving Web site based on a pre-established accept / reject threshold.

The other pilot participants were not successful in enrolling their biometric signatures. Time and resource limitations during Phase 2 of the DMR pilot prevented an analysis that could conclusively attribute to what degree these enrollment failures were due to the rejection of the enrollments by the PenOp program due to unacceptable variation in the signature samples, or to technical problems related to the handling of the large size of the biometric data by software components either on the signer's computer or on the server at the receiving Web site.

In using the plastic stylus and graphics tablet to create the biometric signature, many participants observed that a different signature result seemed to be obtained depending upon whether the signer looked at the graphics tablet or the computer screen while signing. A different result was also obtained depending upon whether the signer executed the signature quickly or whether the signer took care to make sure that the signature fit within the confines of the area on the graphics tablet that recorded the signature.

The vector representation of the signature that was recorded and displayed for reference was recognizable as similar to a pen-and-ink signature by the same person, but in some cases seemed to suggest that the signer may execute a handwritten signature differently when using a stylus and a graphics tablet compared to pen and paper. This result implied that the standard of comparison for a manual authentication of a biometric handwritten signature by a forensic document examiner may need to include data from the set of enrolled signatures as well as a sample of traditional pen-and-ink signatures. In the DMR pilot, the link, or binding, connecting the set of enrolled signatures with the identity of the person depended on elements of the PKI infrastructure previously established in Phase 1. In the DMR pilot, a separate method of binding the identity of the signer to the set of biometric signature samples submitted for enrollment was not explored.

Although the biometric signature method used in Phase 2 of the DMR pilot proved more difficult to implement than the cryptographic signature method used in Phase 1, the pilot participants seemed to intuitively grasp the meaning of the biometric signatures and showed a greater conceptual comfort factor with this natural extension of the more traditional handwritten signature to the signing of electronic documents. The advantage in acceptance and conceptual understanding achieved by linking the biometric handwritten signature to the traditional pen-and-ink handwritten signature used in Western cultures, coupled with adding "something you are" to the security and authentication

dimension to supplement “something you have” and “something you know”, must be compared with the disadvantages posed by the technical challenges, lack of absolute mathematical precision and proprietary implementations of biometric signature methods.

100.1 Results Related to Web-based Reporting

The DMR pilot illustrated the benefits and liabilities of Web-based electronic compliance reporting.

The following benefits of Web-based electronic reporting were illustrated by the pilot:

- Although many of the pilot participants did not have the particular type and version of the Web browser that was selected for the DMR pilot, each pilot participant had used the Web browser that was currently installed on the participant’s computer.
- For those pilot participants behind firewalls implemented by their respective organizations, the participant’s Web browser was already pre-configured to access the Internet through the firewall, and these configurations were preserved during browser upgrades.
- The installation of a Web browser upgrade for use in the DMR pilot provided other benefits to the pilot participants, and therefore was not perceived as the installation of specialized software for the sole purpose of electronic reporting.
- A reasonable expectation exists that maintenance upgrades, security fixes and enhancements, and versions which maintain compatibility with future operating systems will be available free or at low cost for the general-purpose components of a Web-based electronic reporting system.

The following liabilities of Web-based reporting were illustrated by the pilot:

- All of the data volume, security and human interface requirements of electronic reporting must fit within the Web architecture, whether or not this architecture is inherently optimized to meet these requirements.
- The availability of browsers from different manufacturer’s, the large number of versions and maintenance patches of these browsers, the interaction or merging of these browsers with different underlying operating systems, and the multiple ways these browsers can be configured by their end users, contribute to the difficulty of maintaining a controlled software environment on the submitter’s computer.
- To the degree that additional plug-ins, helper applications, separate software applications and / or hardware devices are needed to meet the functional

requirements of the electronic reporting system, the maintenance challenge of achieving and preserving the necessary compatibility among these multiple components increases geometrically.

107.1 Results Related to Electronic DMRs

Electronic DMRs introduce a number of challenges for a Web-based reporting environment. Some of these include:

- Digital signatures must be applied to DMR forms across multiple pages. Since, to be meaningful, a digital signature must be bound to the contents of the document that is signed, the entire contents of the DMR form must be accessible to the software component performing the cryptographic digital signature algorithm or to the cryptographic method used to bind the contents of the form to the biometric signature. This requirement forces multiple-page DMR forms to be loaded from the Web server and processed by an electronic forms plug-in as a single large document, stressing the inherent memory limitations of the browser and the electronic forms plug-in.

- Since a digital signature is bound to the digital representation (not the visual representation) of the electronic form content as it exists in the signer's computer at the time the digital signature is applied, the meaning of the digital signature is lost if the visual representation of the form cannot be reliably linked to its digital representation. The use of an electronic form environment with a de facto history of a reliable correspondence between the visual and digital representation of content, such as Adobe Exchange, introduces the added complexity of a software component from an independent manufacturer that must interact smoothly with its host browser environment. On the other hand, the use of customized enhancements to standard browser functionality, such as ActiveX, Java and JavaScript, introduce a de novo method of linking the visual appearance of a form to its underlying digital representation without the benefit of a body of historical experience to support that this relationship is reliable across browsers, screen sizes and resolutions, and computing platforms.

- The electronic DMR form must allow the entry of multiple rows and columns of data across multiple screen pages without excessive horizontal scrolling while maintaining a readable font size for column headings and parameter limits. Although the bulk of the detailed data verification can be accomplished at the receiving Web site, the electronic DMR form must also make reasonable accommodation for simple data format checking. These human factors impose constraints in the design of the user interface for an electronic DMR that are not as apparent in simpler Web-based forms, such as electronic commerce shopping carts.

In the DMR pilot, the participants clearly intuitively understood and were comfortable with the user interface provided by the Adobe Acrobat Exchange form plug-in. [Detailed comments from the pilot participants related to the user interface have been discussed previously in Section 3.3, Reactions of Pilot Participants.]

The Adobe Acrobat Exchange electronic form environment also allowed both the cryptographic and biometric digital signature software components, implemented as plug-ins to the Adobe Exchange form, to have access to the complete form content (template and submitted data) in order to bind the digital signature to this content at the time of signing.

The Adobe Exchange electronic form environment also enhanced the meaningfulness of the digital signature by the de facto history of the Adobe Exchange product in faithfully rendering the content of the form across a wide variety of computer platforms. In other words, a reasonable case could be made that the correspondence between the visual representation of the form and its digital representation was standard and reliable.

The Adobe Exchange form allowed simple data verification rules, data format masks and tab order to be built into the form. The Adobe Exchange application could be used to print a copy of the DMR form with a content representation identical to the screen display.

In the DMR pilot, the following disadvantages were observed in the use of the Adobe Exchange form, implemented as a plug-in to a Web browser, as the electronic form environment for the DMR:

- The Adobe Exchange form introduced the complexity and cost of another manufacturer's product into the Web-based reporting architecture.
- The Adobe Exchange application behaved differently as a plug-in to Microsoft Explorer vs. Netscape Navigator when used in conjunction with the HAHTsite application server.
- Adobe Exchange, as a single-tasking application, did not behave properly if more than one instance was launched on the same computer.
- Adobe Exchange introduced additional memory limitations above those introduced by the Web browser.
- A window for the Adobe Exchange application automatically opened and needed to be minimized by the user even though the form content was displayed in the browser's user interface.
- The color and appearance of the Adobe Exchange form was affected by the digital signature plug-ins when participant's computer was configured for certain screen resolutions.

- The Adobe Exchange form occasionally did not load pre-populated form data if another memory-intensive application had been recently used.
- The Adobe Exchange form introduced the need to make additional configuration settings if the Web browser type was changed.
- The use of the Adobe Exchange form added complexity to the programming of the application server within the receiving Web site.
- The use of the Adobe Exchange form introduced the need for an additional software installation step from an Adobe distribution CD.
- The Adobe Exchange plug-in must be re-installed if the Web browser is re-installed.

In summary, the use of the Adobe Exchange form plug-in to the Web browser effectively solved a number of difficult and significant digital signature and human interface problems in implementing an electronic version of the DMR form. The introduction of the Adobe Exchange form also added a number of technical problems and complexities to the electronic reporting system.

122 Conclusions

Summary conclusions that could be drawn from experience with the DMR pilot in the State of New York include:

An effective, low-cost, and scaleable public key infrastructure (PKI) for the purpose of certificate management can be established and operated with relative ease by even a small compliance program.

A requirement for a digital signature of legal significance that can be strongly authenticated and supported in a court of law arguably imposes requirements on the design of an electronic reporting system above and beyond the authentication mechanisms commonly accepted as adequate for routine consumer electronic commerce on the Internet.

The most difficult technical challenges in implementing an electronic reporting system with strong digital signatures occur in the software

components needed to create an electronic form interface and execute a digital signature on the submitter's computer.

If hardware and software components in addition to the Web browser are used to meet electronic form user interface or digital signature requirements, the amount of technical support required to install and maintain the electronic reporting system on each submitter's computer is geometrically proportional to the number of such added components.

The behavior of software products vary dramatically when used in an integrated system in combination with slightly different versions or types of other products and operating systems. Each different configuration therefore requires extensive testing and tailored technical support.

Cryptographic digital signatures typically succeed once the initial investment has been made in installing the software components and completing the certificate registration process. However, the one-time installation, set-up and certificate registration can be time consuming and subject to multiple failure modes.

Biometric handwritten digital signatures pose unique technical challenges and were less successful than cryptographic signatures in the DMR pilot, although the pilot participants found biometric handwritten signatures conceptually easier to understand.

The use of Adobe Exchange as a Web browser plug-in produced an electronic environment for the DMR form that was immediately and intuitively understood by the pilot participants. Adobe Exchange also facilitated the implementation of a strong digital signature with legal

significance. However, the introduction of Adobe Exchange into the electronic reporting system also introduced problems related to the handling of memory and compatibility with other software components.

Strong security and digital signature requirements dramatically increase the installation, setup and technical support time needed to implement the electronic reporting system. Conversely, incrementally relaxing these requirements would be predicted to incrementally reduce installation, setup and installation time. However, with relaxed requirements the risk increases that the electronically submitted DMR form may not be able to be legally attributed to its submitter.